LIGHTWEIGHT CRYPTOGRAPHIC TECHNIQUES

Horace Yuen, Alan Sahakian *Northwestern University*

Agnes Chan *Northeastern University*

Majid Sarrafzadeh *UCLA*

PROBLEMS

- Information security in microsensor networks
  - authentication < identification, data integrity
  - encryption
  - key management
- Performance Measures:
  1. Security level
  2. Power consumption
  3. Encryption/decryption rate
  4. Complexity/cost

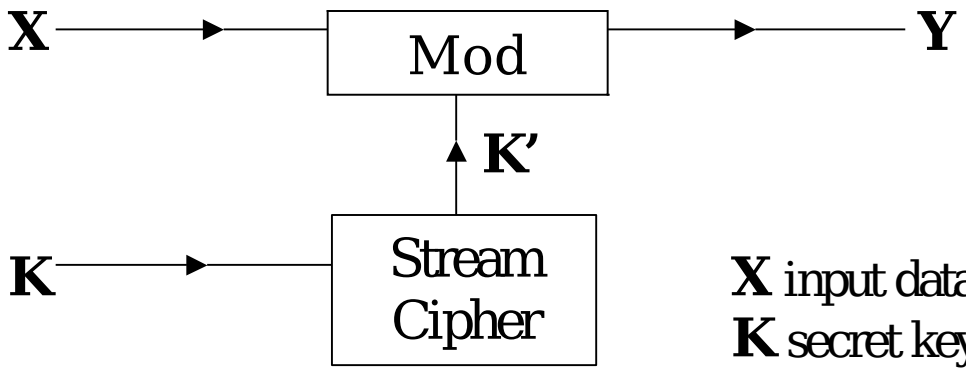
Tasks:

A. Novel Stream Ciphers

B. New Spread Signal (SSi) Cryptography

C. Power Efficient Cryptoalgorithms

Encryption Secrecy



X input data
K secret key
K' running key
Y output data

- K' **not observable –**

  no known-plaintext attack can be launched against the stream cipher; exponential search needed to find K

- **Protect against known-plaintext attack for the above SSi scheme via Data Randomization–**

  use two systems with inputs X **and** X + X~ **,**

  X **random**

UNDERLYING MECHANISM

Error prob $P_e \sim \exp\{ -SNR / 2 \}$

in additive white Gaussian noise

SNR signal-to-voice ratio

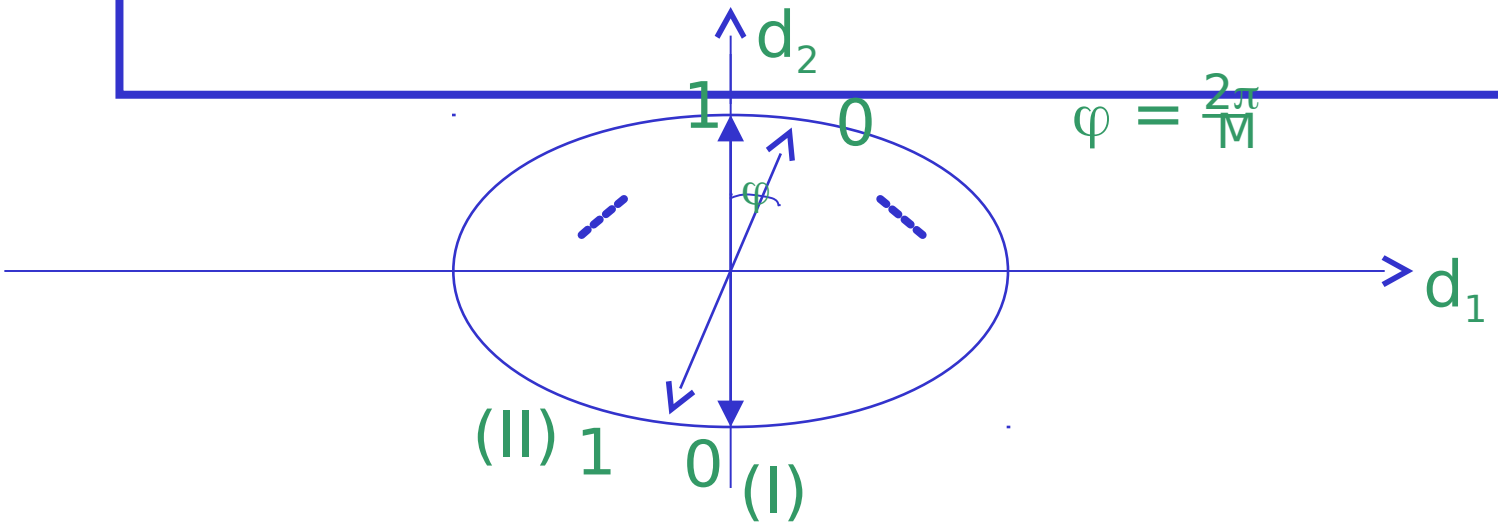
- $SNR_B = E_0/N_0$ for Babe
- $SNR_1 = E_1/N_1$ for Eve

if basis known

- $SNR_M =$ *if basis unknown*

➢ Can utilize deliberate randomization in lieu of channel noise

M-ARY PHASE SHIFT KEYING (BPSK)



- basis I or II or . . . (M/2)

  known to users **A** and **B** as **BPSK**

- basis unknown to eavesdropper **E**

Eve

Task C: Power Efficient Cryptoalgorithms

- **Predictability Driven Low Power Design Methodology**

- **Improving the design tolerance to uncertainties**

Predictability Driven Design Flow

- **Definition:** Quantified value of (in)accuracy is defined as (un)predictability.

- **Causes:**
  - Downstream Optimizations: The correct position of a node on the power/delay, power/area curve is not known at high level causing unpredictability
  - Input Trace: The application that runs on the design can greatly effect the power estimate
  - Unawareness of module architecture
  - Other sources: Physical Design, glitch etc.

Predictability Driven Design Flow

- **Why is Predictability Important?**

A More Predictable Design would mean more accurate and meaningful estimates

Enables the development of a system that has accuracy/design quality tradeoff

Predictability Driven Design Flow

Arch.	Option1	Option2	Option3	Option4	Option5	Avg	Max Variation
arch1	12.89	12.09	14.09	19.38	14.09	14.5	33.6%
arch2	15.22	13.99	17.38	17.47	17.38	16.3	14.05 %

- The table indicates the variation of power for different optimization scripts of design compiler for two different architectures

- It indicates that even though arch2 dissipates more power, it has higher predictability

Tradeoff Between Design Quality and Predictability

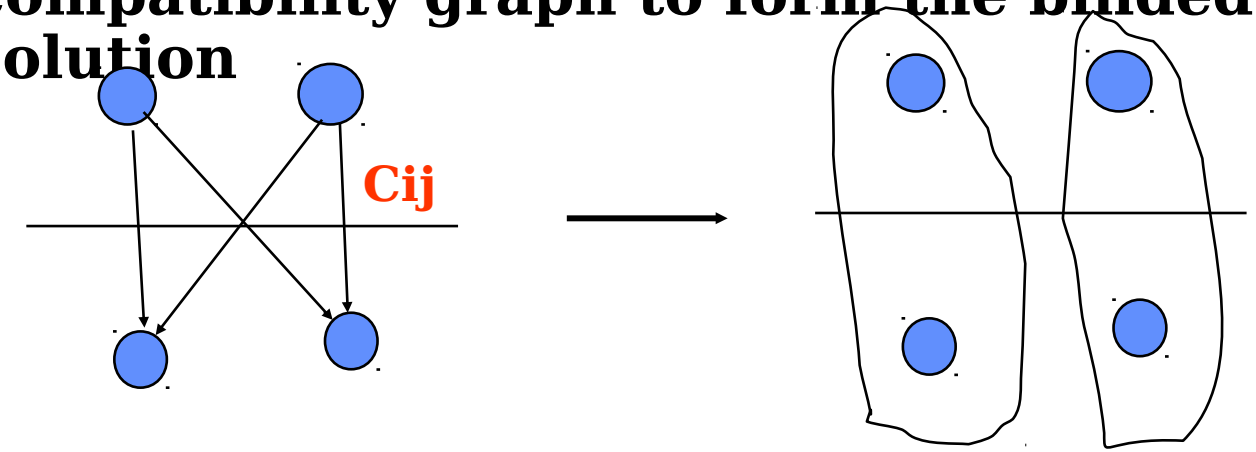
Predictability Driven Design Flow

	arch1	arch2	Average	Variation
Option1	13.23	17.85	15.54	14.8%
Option2	12.23	17.74	15.06	17.99%
Option3	14.4	14.3	14.35	0.3%
Option4	19.73	15.35	17.54	10.8%

- This table indicates the variation in the power dissipation for different architecture and different optimization options
- Hence if we don't know the architecture that implements a computation that can also lead to unpredictability

Predictability Driven Binding

- **Low Power Binding Problem has been optimally solved using Min-Cost flow methodology (or ILP formulations)**
- **It Minimizes the sum the switched capacitance of all the edges used in the compatibility graph to form the binded solution**



Compatibility Graph: All edges have costs that indicate the associated switching activity

Binded Solution

Predictability Driven Design Flow

- **Let us assume each edge cost of the compatibility graph has an associated unpredictability. These unpredictabilities are represented as % variation from the base cost value**
- **The objective is to minimize the unpredictability of the binded solution**
- **Objective Functions:**
  - **Average of the unpredictability of the edges in the binded solution is minimized**
  - **Maximum unpredictability in the binded solution is minimized**

Predictability Driven Design Flow

Some Experimental Results

- **Benchmarks: Mediabench (C)**
- **SUIF was used to generate DFGs which were scheduled with a path based scheduler.**
- **The DFG was then characterized for switched capacitance and unpredictability using synopsis D.C.**
- **It was then binded using different objective functions: Mincost (Minimum switched capacitance), Min Average Unpredictability and Min Max Unpredictability**

Predictability Driven Binding: Experimental Results

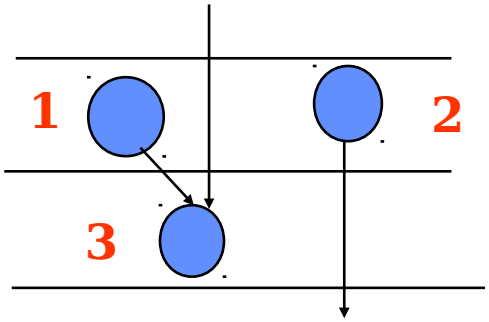
Bench	Objective: Cost		Objective: Avg Unpred		Objective: Max Unpred	
	Cost	Unpred	Cost	Unpred	Cost	Unpred
fft2	76.57	0.27	98.31	0.18	89.76	0.18
jctrans 1	159.99	0.33	173.12	0.11	173.3 2	0.12
jctrans 2	42.10	0.29	48.96	0.11	51.14	0.12

- We see that an unpredictability driven binding methodology greatly improves the level of accuracy as compared to a Mincost solution (Minimum power solution)

Uncertainty Driven Design Flow

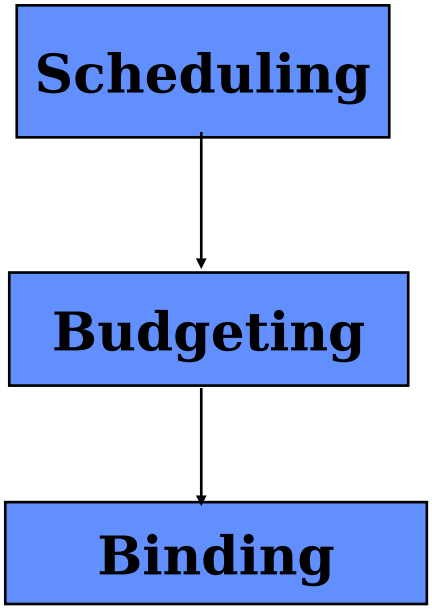
- The idea is to have a high level specification of the design which allows a lot of freedom to low level optimizations
- This freedom can be generated by exploiting the concept of slack in high level designs
- More slack would make the design robust to uncertainties
- More slack will enable better design space exploration by low level optimizations

Slack Oriented Design Flow



- Operation 2 can be scheduled in either clock step 1 or 2
- This extra slack can be used by delaying operation 2, hence gaining in area/power/runtime. It makes the design tolerant to uncertainties.
- Experiments with synopsis design compiler shows that this extra slack can make logic synthesis 50% faster.

Slack Oriented Design Flow



Scheduling for more slack, Independent Set Based Algorithm

Delay Budgeting for Maximum Slack Utilization: Optimally Solvable

Binding operations for generatingresources with high slack

Slack Oriented Design Flow

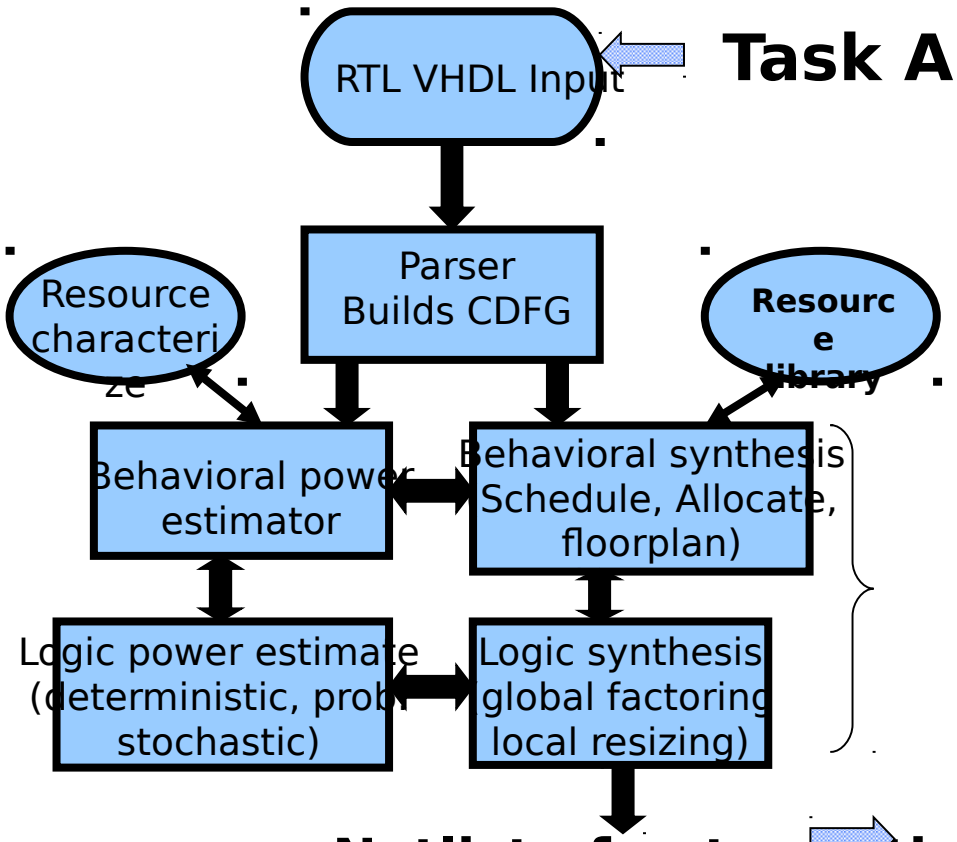
- **Experimental results showed that for some typical benchmarks generated from the Mediabench Suite, we could generate a binded solution with resoureces having relaxed delay constraints due to higher slacks**

- **These relaxed delay constraints could be used by the low level logic optimization tools to improve the design quality and runtime.**

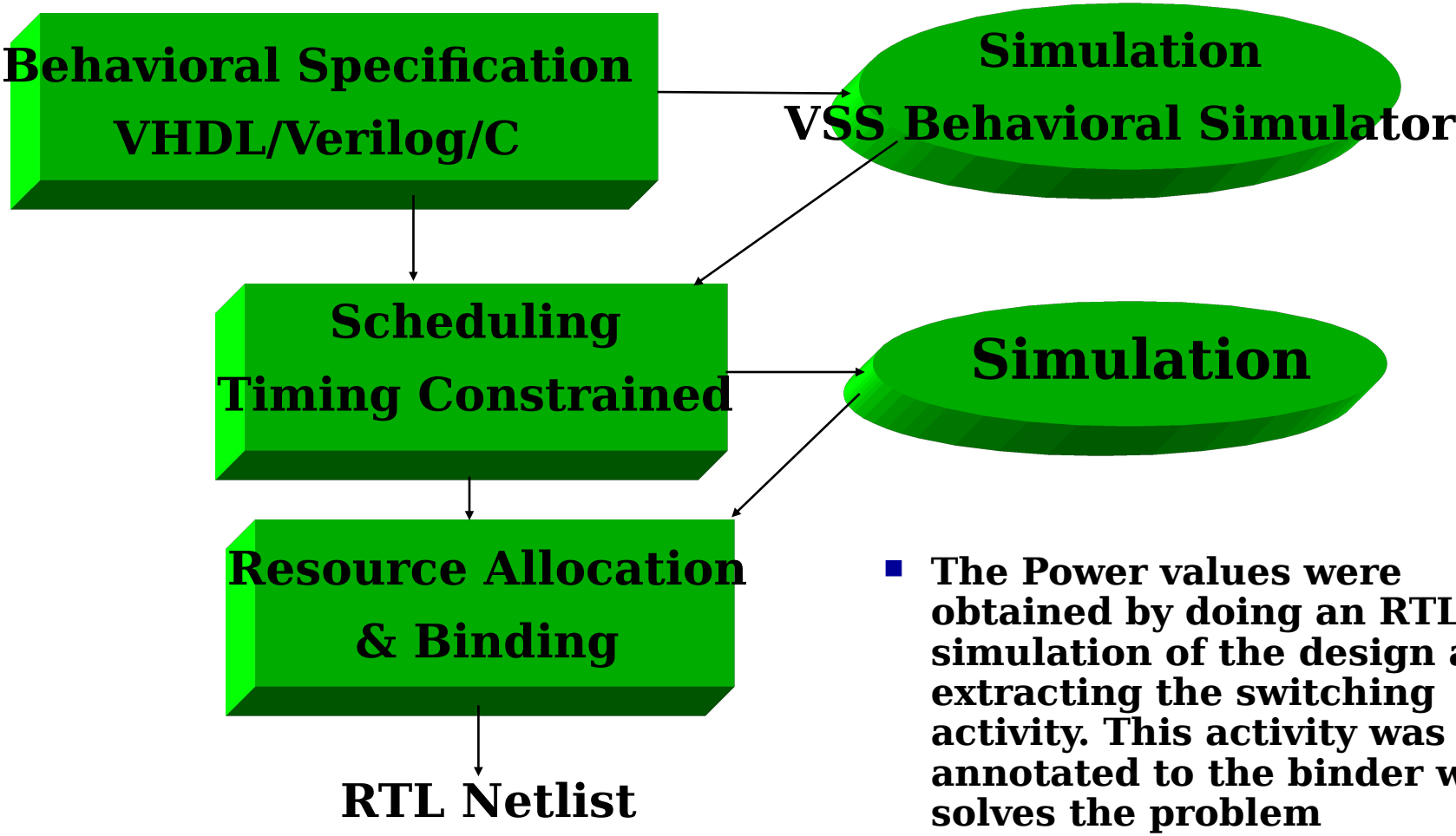
Benchmarking: Cryptography

- **VHDL/ C implementations of Crypto-algorithms are being studied for power/security tradeoffs.**
- **Emphasis on sensor network kind of applications where power needs to be saved keeping some degree of security. Or, to tradeoff security/power/cost**
- **Study of predictability issues in crypto-hardware**

Power Efficient Cryptoalgorithms

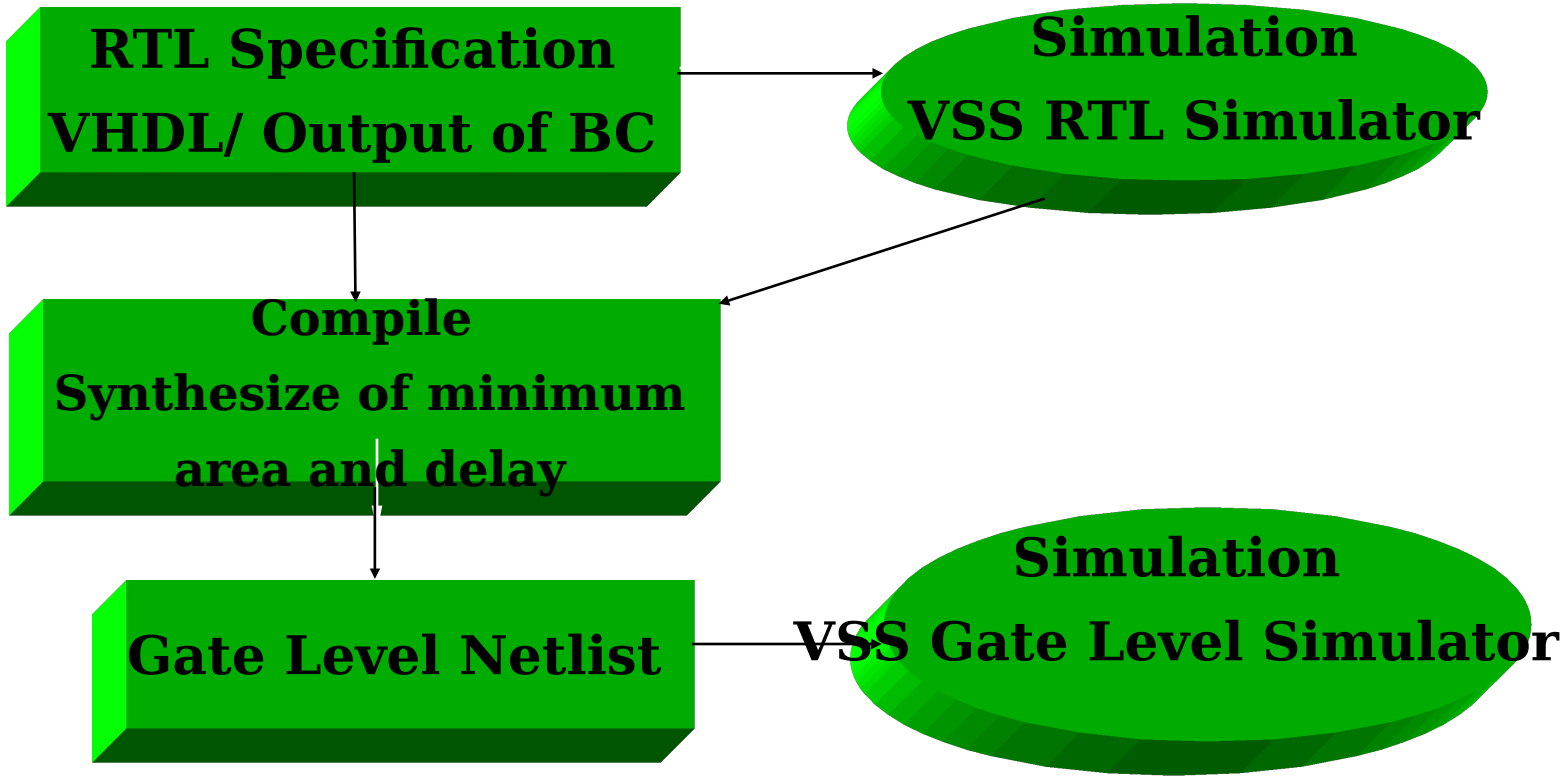


Power Driven High Level Design Flow



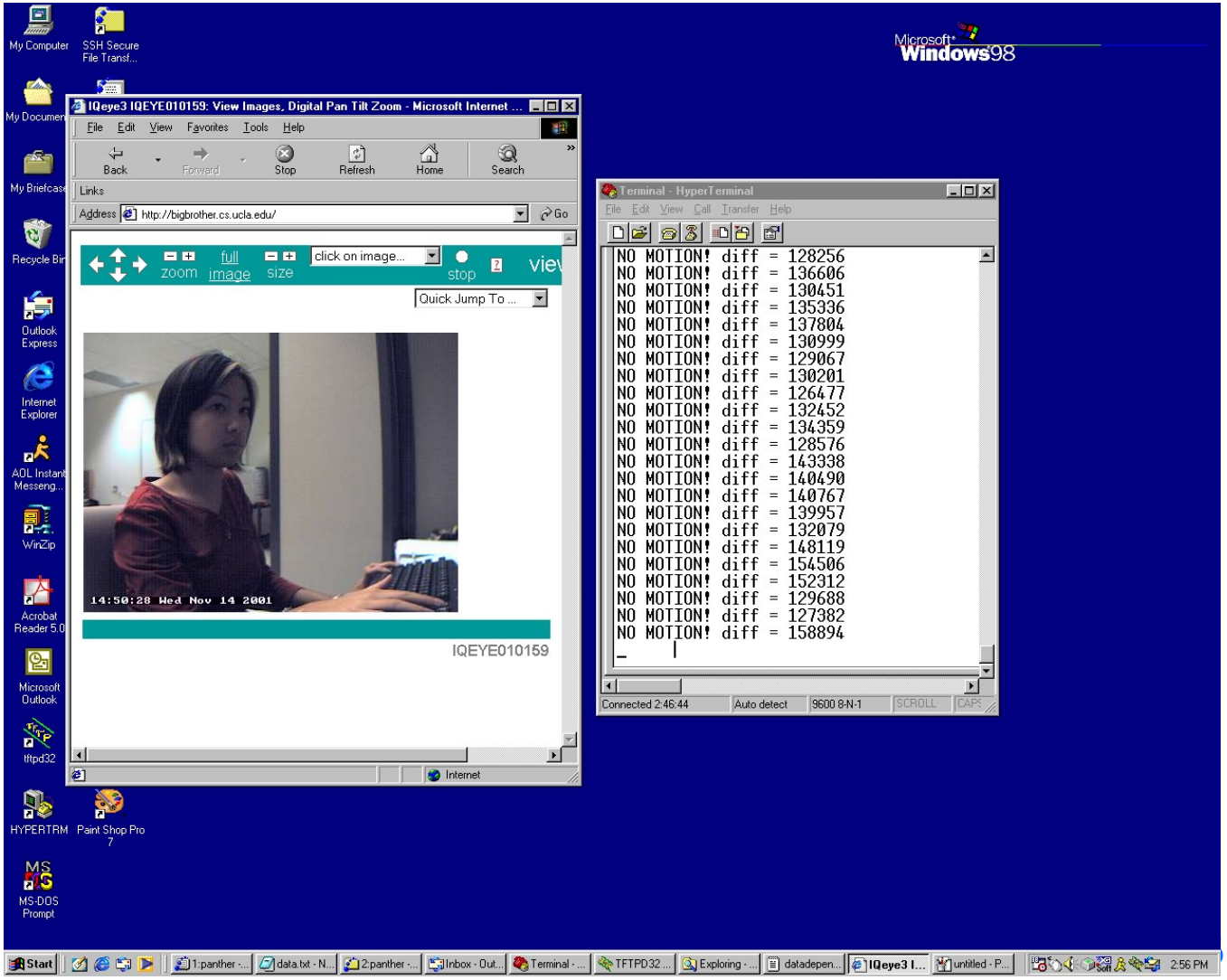
- The Power values were obtained by doing an RTL simulation of the design and extracting the switching activity. This activity was annotated to the binder which solves the problem

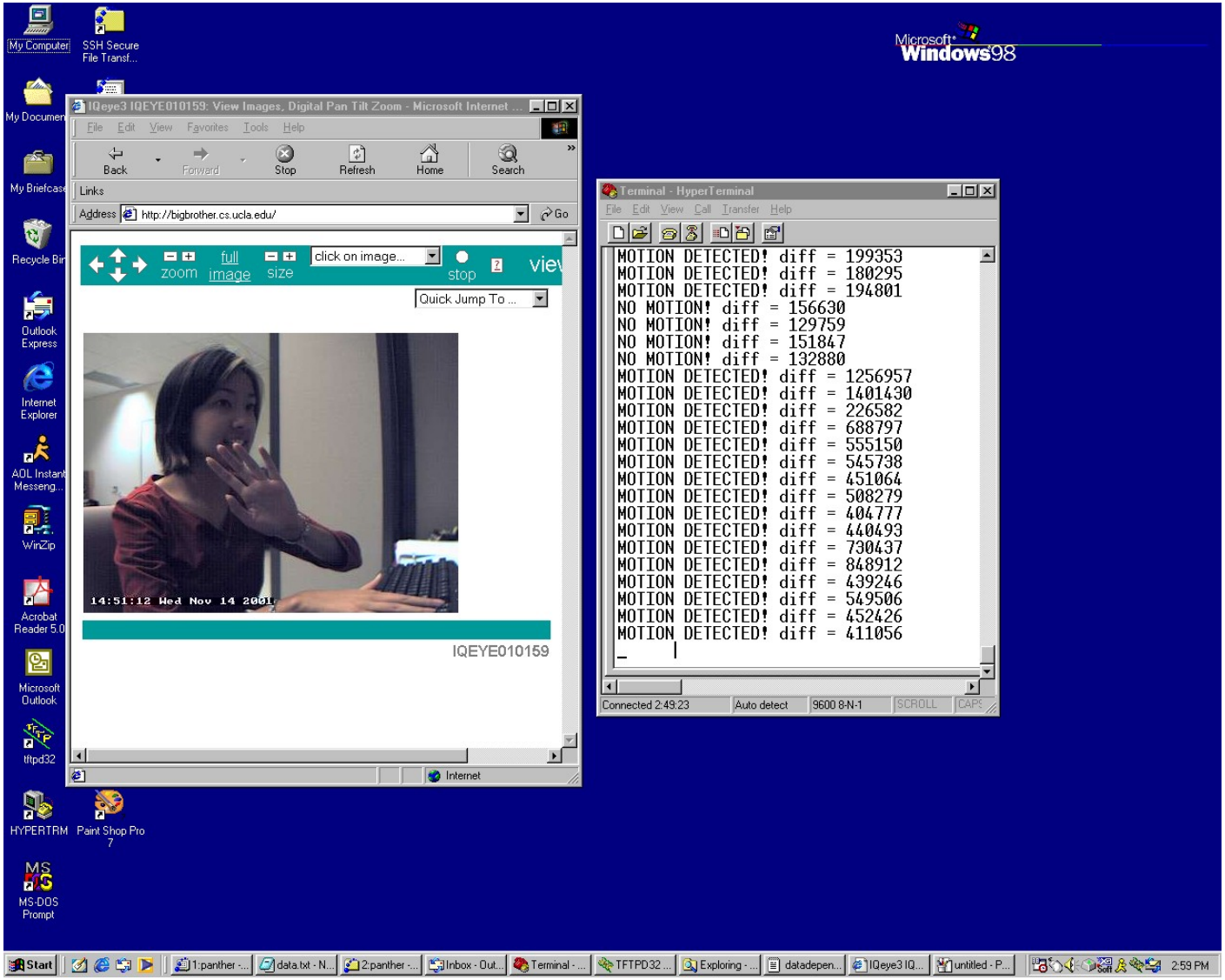
Power Driven At RT-Level and Gate Level (Synopsis DC)



- **Crypto-motion tracking/estimation**

Example


My Computer
SSH Secure File Transf...
My Documents
My Briefcase
Recycle Bin
Outlook Express
Internet Explorer
AOL Instant Messeng...
WinZip
Acrobat Reader 5.0
Microsoft Outlook
tftpd32
HYPERTRM
Paint Shop Pro 7
MS-DOS Prompt
Microsoft Windows 98
IQeye3 IQEYE010159: View Images, Digital Pan Tilt Zoom - Microsoft Internet ...
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search
Links
Address http://bigbrother.cs.ucla.edu/
Go
zoom full image size
click on image...
stop
Quick Jump To ...
14:50:28 Wed Nov 14 2001
IQEYE010159
Internet
Terminal - HyperTerminal
File Edit View Call Transfer Help
NO MOTION! diff = 128256
NO MOTION! diff = 136606
NO MOTION! diff = 130451
NO MOTION! diff = 135336
NO MOTION! diff = 137804
NO MOTION! diff = 130999
NO MOTION! diff = 129067
NO MOTION! diff = 130201
NO MOTION! diff = 126477
NO MOTION! diff = 132452
NO MOTION! diff = 134359
NO MOTION! diff = 128576
NO MOTION! diff = 143338
NO MOTION! diff = 140490
NO MOTION! diff = 140767
NO MOTION! diff = 139957
NO MOTION! diff = 132079
NO MOTION! diff = 148119
NO MOTION! diff = 154506
NO MOTION! diff = 152312
NO MOTION! diff = 129688
NO MOTION! diff = 127382
NO MOTION! diff = 158894
Connected 2:46:44
Auto detect
9600 8-N-1
SCROLL
CAPS
Start
2:56 PM


My Computer
SSH Secure File Transf...
My Documents
My Briefcase
Recycle Bin
Outlook Express
Internet Explorer
AOL Instant Messeng...
WinZip
Acrobat Reader 5.0
Microsoft Outlook
tftpd32
HYPERTRM
Paint Shop Pro 7
MS-DOS Prompt
Microsoft Windows98
IQeye3 IQEYE010159: View Images, Digital Pan Tilt Zoom - Microsoft Internet ...
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search
Links
Address http://bigbrother.cs.ucla.edu/
Go
zoom full image size
click on image...
stop
Quick Jump To ...
14:51:12 Wed Nov 14 2001
IQEYE010159
Internet
Terminal - HyperTerminal
File Edit View Call Transfer Help
MOTION DETECTED! diff = 199353
MOTION DETECTED! diff = 180295
MOTION DETECTED! diff = 194801
NO MOTION! diff = 156630
NO MOTION! diff = 129759
NO MOTION! diff = 151847
NO MOTION! diff = 132880
MOTION DETECTED! diff = 1256957
MOTION DETECTED! diff = 1401430
MOTION DETECTED! diff = 226582
MOTION DETECTED! diff = 688797
MOTION DETECTED! diff = 555150
MOTION DETECTED! diff = 545738
MOTION DETECTED! diff = 451064
MOTION DETECTED! diff = 508279
MOTION DETECTED! diff = 404777
MOTION DETECTED! diff = 440493
MOTION DETECTED! diff = 730437
MOTION DETECTED! diff = 848912
MOTION DETECTED! diff = 439246
MOTION DETECTED! diff = 549506
MOTION DETECTED! diff = 452426
MOTION DETECTED! diff = 411056
Connected 2:49:23
Auto detect
9600 8-N-1
SCROLL
CAPS
Start
1:panther -...
data.txt - N...
2:panther -...
Inbox - Out...
Terminal - ...
TFTPD32 ...
Exploring - ...
datadepen...
IQeye3 IQ...
untitled - P...
2:59 PM

FUTURE WORK

- Tradeoff of the various performance measures and system parameters for different modulation/encryption formats
- Quantify security levels, via Eve's probabilities of successful estimating the data and the key, as functions of system parameters
- Complete security proofs